Sicheres DFNRoaming in der Fraunhofer-Gesellschaft

Peter Zimmer

Fraunhofer NOC
Fraunhofer Institut IITB
Fraunhoferstraße 1
76131 Karlsruhe
peter.zimmer@iitb.fraunhofer.de

Abstract: Die Fraunhofer-Gesellschaft ist seit Anfang 2007 Nutzer des DFNRoaming-Dienstes des DFN-Vereins. Aufgrund des hierarchischen Aufbaus des Dienstes innerhalb von Fraunhofer mit einem zentralen Übergangspunkt zum DFNRoaming wird die Umsetzung des Dienstes innerhalb der Fraunhofer-Gesellschaft *Fraunhofer-Roaming* genannt. Durch Fraunhofer-Roaming wird den Fraunhofer-Mitarbeitern die Möglichkeit gegeben, sich an allen am DFNRoaming teilnehmenden Einrichtungen mit ihren persönlichen Benutzerdaten anzumelden und so einen Internetzugang zu erhalten.

Bei der im Fraunhofer-Roaming verwendeten Authentifizierung mittels Web-Redirect können die Benutzerpassworte von allen an der Authentifizierung beteiligten Knoten im Klartext eingesehen werden. Aufgrund dieser Problematik verwendet Fraunhofer-Roaming Einmal-Passworte, die zentral gespeichert sind.

Dieser Artikel beschreibt die Implementierung des Fraunhofer-Roaming und gibt einen Ausblick auf die weitere Entwicklung in diesem Gebiet.

1 Motivation

Die Fraunhofer-Mitarbeiter betreiben einen sehr starken wissenschaftlichen Austausch mit nationalen und internationalen Forschungseinrichtungen.

Bei ihrem Besuch in einem Fraunhofer-Institut haben die Mitarbeiter aus den befreundeten Forschungseinrichtungen die Möglichkeit mittels eines Gast-Tickets einen Internet-Zugang zu erhalten. Das Verfahren für einen Fraunhofer-Mitarbeiter bei seinen Dienstreisen in den befreundeten Forschungseinrichtungen einen Internet-Zugang zu erhalten, sind sehr unterschiedlich.

Der DFN-Verein bietet als Internet-Provider für zahlreiche deutsche Forschungseinrichtungen mit DFNRoaming einen deutschlandweiten Authentifizierungsverbund, an dem DFN-Mitglieder kostenlos teilnehmen können. DFNRoaming erlaubt den Mitarbeitern der teilnehmenden Einrichtungen, mit ihren persönlichen Zugangsdaten und ohne weitere Beantragung in einer anderen teilnehmenden Einrichtung einen Internet-Zugang zu erhalten.

Die Fraunhofer-Gesellschaft nimmt seit Anfang 2007 am DFNRoaming teil. Damit wird das Verfahren zur Erlangung eines Internet-Zugangs in einer der teilnehmenden Einrichtung für die Fraunhofer-Mitarbeiter standardisiert. Im Gegenzug wird für Gäste aus diesen Einrichtungen die Notwendigkeit eines Gast-Tickets beseitigt.

Das *Fraunhofer Network Operations Center (NOC)* ist für die Anbindung der Fraunhofer-Gesellschaft an DFNRoaming verantwortlich. Innerhalb der Fraunhofer-Gesellschaft wurde Fraunhofer-Roaming implementiert, das eine ähnliche Struktur wie DFNRoaming innerhalb der Fraunhofer-Gesellschaft realisiert. Der Übergang zum DFN-Verein wird über einen zentralen Knoten bewerkstelligt. Abbildung 1 zeigt die logische Struktur der Anbindung. Die Fraunhofer-Institute sind an einen zentralen Knoten angebunden, der seinerseits die Verbindung zum DFN herstellt.

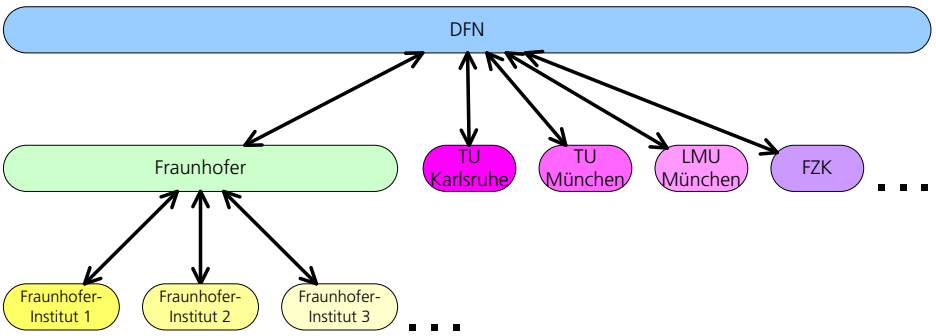


Abbildung 1: Einbettung der Fraunhofer-Gesellschaft in DFNRoaming

Das nachfolgende Kapitel beschreibt die Realisierung von Fraunhofer-Roaming sowohl des zentralen Knotens als auch in den Fraunhofer-Instituten. Diese Beschreibung dient als Grundlage für die weiteren Sicherheitsbetrachtungen in Kapitel 3. Dort werden die Sicherheitsrisiken einer deutschlandweiten Authentifizierung beleuchtet, woraus einige Schlüsse für die Umsetzung gezogen werden. Kapitel 4 beschreibt die Realisierung des verwendeten Einmal-Passwort-Mechanismus. Der jetzige Entwicklungsstand stellt den ersten Schritt zur Realisierung einer durch die modernsten Sicherheitstechniken abgesicherten weltweiten Authentifizierung in der Fraunhofer-Gesellschaft dar. Techniken wie 802.1x oder das gerade formierende Shibboleth werden derzeit noch nicht unterstützt. Kapitel 5 gibt einen kurzen Ausblick auf die weiteren Aktivitäten innerhalb der Fraunhofer-Gesellschaft in diesem Gebiet.

2 Realisierung

In diesem Kapitel wird die Realisierung der zentralen Authentifizierung innerhalb der Fraunhofer-Gesellschaft (Fraunhofer-Roaming) mit Anbindung an DFNRoaming beschrieben.

Fraunhofer-Roaming basiert wie DFNRoaming auf dem RADIUS-Protokoll, das in Abschnitt 2.1 kurz eingeführt wird. In Abschnitt 2.2 wird die Netzwerkstruktur eines Fraunhofer-Institutes vorgestellt. Darauf aufbauend wird in Abschnitt 2.3 die Implementierung der Fraunhofer-weiten Authentifizierung beschrieben.

2.1 Das RADIUS-Protokoll

Das *Remote Dial-In User Service (RADIUS)*-Protokoll [2], [3] ist ein Protokoll zu Authentifizierung, Autorisierung und Accounting von Benutzern. Im hier vorliegenden Kontext von Fraunhofer-Roaming und DFNRoaming wird ausschließlich die Authentifizierung von Benutzern verwendet. RADIUS ist eine Client-Server Architektur, d.h. ein Client stellt eine Authentifizierungsanfrage und ein RADIUS-Server beantwortet diese positiv oder negativ.

Bei den Roaming-Verfahren werden sogenannte *RADIUS-Proxys* eingesetzt, die eine Authentifizierungsanfrage nicht selbst beantworten, sondern diese an einen weiteren RADIUS-Server weiterleiten. Damit entsteht eine Authentifizierungskette von RADIUS-Servern. Am dem einen Ende der Kette steht der Benutzer, der eine Authentifizierung wünscht und am anderen Ende ein RADIUS-Server, der die Anfrage bearbeitet.

Eine Authentifizierungsanfrage besteht aus einem Benutzernamen und einem Passwort. Der Benutzername setzt sich wie folgt zusammen:

<User>@<REALM>

User ist eine klassische UID, die dem Benutzer zugeordnet ist. Der *REALM* ist der Bezeichner für eine Authentifizierungsdomäne. Die hier vorgestellten Roaming-Verfahren benutzen den REALM, um eine Authentifizierungsanfrage einer Institution zuzuordnen und damit die Authentifizierungsanfrage korrekt weiterzuleiten.

Bekannte RADIUS-Server sind FreeRADIUS [4] und RADIATOR [5]. In der Fraunhofer—Gesellschaft kommt RADIATOR zum Einsatz. Diese beiden RADIUS-Server bieten zahlreiche Anbindungen an weitere Authentifizierungsmethoden wie z.B. EAP-TTLS, das bei 802.1x [7] eingesetzt werden kann.

2.2 Das Netzwerk bei einem Fraunhofer-Institut

Abbildung 2 zeigt die Netzwerkstruktur eines Fraunhofer-Institutes. Durch eine zentrale Firewall werden 6 Sicherheitszonen realisiert, die voneinander weitestgehend abgeschirmt sind. In einer Sicherheitszone sind Rechner mit gleichem oder ähnlichem Sicherheitsanspruch platziert. Der Übergang zwischen den Sicherheitszonen ist durch das IT-Sicherheitshandbuch der Fraunhofer-Gesellschaft geregelt.

Das *Public-LAN* ist die Implementierung einer DMZ, die eine Substrukturierung in weitere Sicherheitsstufen aufweist. Damit können die angebotenen Dienste gegen Angriffe von anderen Rechnern aus der DMZ geschützt werden. Details hierzu sind in [1] beschrieben.

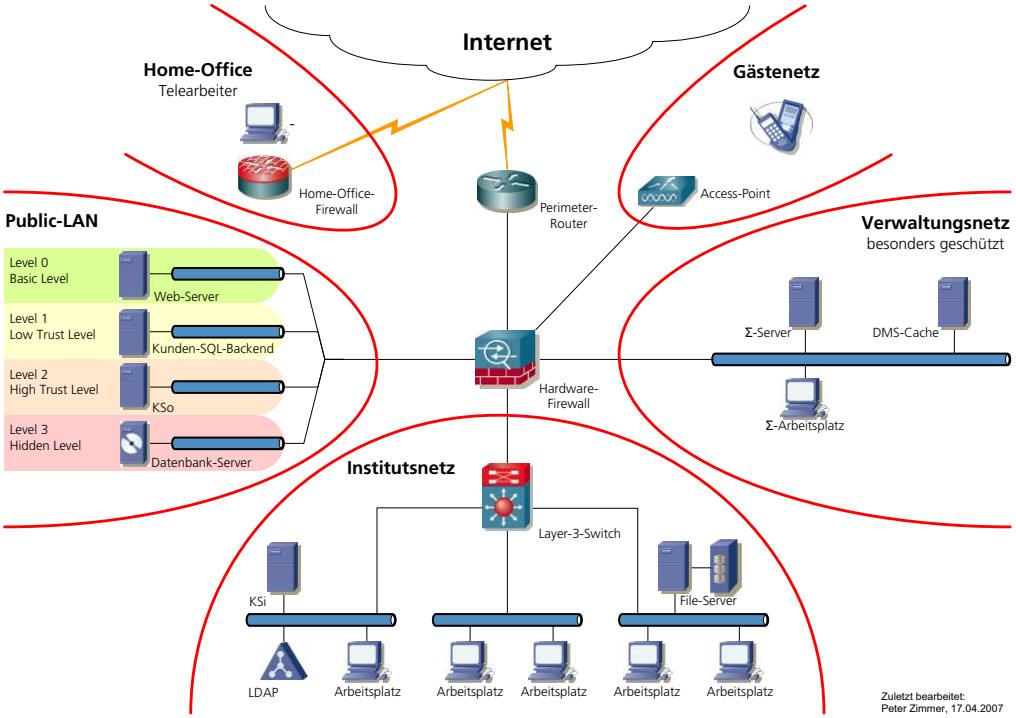


Abbildung 2: Netzwerkstruktur eines Fraunhofer-Institutes

Im *Institutsnetz* sind die Arbeitsplätze des Institutes platziert. Hier ist je nach Institut eine Unterteilung in weitere Sicherheitsbereiche vorgenommen, die Unterteilung liegt in Hoheit des Institutes.

Das *Verwaltungsnetz* stellt einen besonders geschützten Bereich innerhalb des Netzwerkes dar. Dort sind die Verwaltungs-Rechner platziert, z.B. alle Rechner, die in Lohn- und Finanzverwaltung eingesetzt werden. Die Verwaltungsnetze aller Institute sind über VPN-Tunnel mit den zentralen Verwaltungsservern der Fraunhofer-Zentrale in München verbunden.

Das *Gästenetz* ist ein Sicherheitsbereich, in dem alle institutsfremden Rechner platziert werden. Im Allgemeinen sind dies Laptops, die per WLAN einen Internetzugang erhalten. Soll ein Gast einen Internet-Zugang erhalten, dann kann er ein GastTicket verwenden, das durch das Institut ausgestellt wird.

Verbinden sich Institutsmitarbeiter von zu Hause aus mit dem Institut, werden diese in den Sicherheitsbereich *Home-Office* untergebracht. Von dort aus sind alle notwendigen Zugriffe auf die Institutsressourcen erlaubt, einige kritische Zugriff werden aber geblockt. Außerdem werden die Zugriffe protokolliert.

Die Sicherheitszonen *Verwaltungsnetz*, *Institutsnetz*, *Public-LAN* und *Internet* bilden eine Kette mit absteigender Sicherheitseinstufung. Das Gästenetz und das Home-Office werden von der Sicherheit her wie das Internet eingestuft. Prinzipiell sind Zugriffe nur von sicheren Bereichen in unsicherere Bereiche gestattet. Zugriffe aus einem Sicherheitsbereich in einen sichereren Bereich werden in der Firewall einzeln freigeschaltet und dokumentiert. Diese bedürfen der Genehmigung durch den IT-Sicherheitskoordinator der Fraunhofer-Gesellschaft.

2.3 Fraunhofer-weite RADIUS-Authentifizierung

Das Fraunhofer-NOC betreibt zwei zentrale RADIUS-Server (radius1.fraunhofer.de, radius2.fraunhofer.de), die als RADIUS-Proxys die Authentifizierungsanfragen je nach REALM weiterleiten.

In den Fraunhofer-Instituten werden zwei sogenannte Kommunikationsserver betrieben. Im Public-LAN (Level 2) ist der *äußere Kommunikationsserver KSo* untergebracht und im Institutsnetz ist der *innere Kommunikationsserver KSi* installiert. Die Kommunikationsserver erbringen gemeinsam Kommunikationsdienste, die die Wissenschaftler bei ihrer täglichen Arbeit unterstützen (z.B. DNS, E-Mail, Internet-Access, VPN-Access). Auf den Kommunikationsservern ist jeweils ein RADIATOR installiert.

Die RADIUS-Server auf den Kommunikationsservern sind neben Fraunhofer-Roaming für die Authentifizierung beim VPN-Access (für das Home-Office) sowie der Gast-Tickets (für das Gäste-Netz) zuständig. Mit der Einführung der Fraunhofer-Roaming durften diese beiden Dienste nicht beeinträchtigt werden.

Die RADIUS-Server auf den Kommunikationsservern sind so konfiguriert, dass alle Anfragen ohne REALM (z.B. zm) lokal im Institut behandelt werden. Leere REALMS (NULL-REALM) werden bei der Authentifizierung für den VPN-Access und den Gast-Tickets verwendet. Ist ein REALM vorhanden, werden die Anfragen vom KSi zum KSo weitergeleitet und von dort zu den zentralen RADIUS-Servern der Fraunhofer-Gesellschaft.

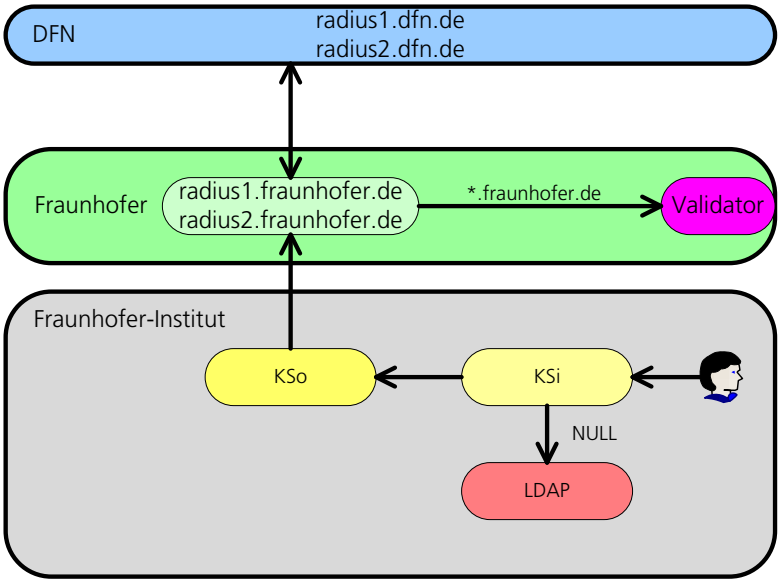


Abbildung 3: Ablauf einer Authentifizierung

Abbildung 3 zeigt den Ablauf einer Authentifizierung abhängig vom REALM der Anfrage. Der Benutzer stellt über das Authentifizierungsgerät (zumeist Cisco PIX/ASA Firewall) eine Authentifizierungsanfrage an den KSi des Institutes. Wird die Anfrage mit dem NULL-Realm (ohne @) gestellt, dann wird die lokale Authentifizierungsdatenbank des Institutes zur Authentifizierung benutzt. Alle anderen Authentifizierungen werden an den KSo weitergeleitet, der diese an die zentralen RADIUS Server radius1.fraunhofer.de und radius2.fraunhofer.de weiterleitet. Lautet der REALM auf *.fraunhofer.de, wird der Fraunhofer-Validator (roaming.noc.fraunhofer.de) zur Authentifizierung benutzt. Alle anderen Anfragen werden an die RADIUS Server des DFN weitergeleitet.

3 Was ist mit Sicherheit?

Möchte ein Fraunhofer-Mitarbeiter in einer am DFNRoaming teilnehmenden Einrichtung einen Internet-Zugang erhalten, verbindet er sich mit dem WLAN mit der SSID VPN/WEB und versucht eine beliebige Webseite mit seinem Browser zu erreichen. Das zwischengeschaltete Authentifizierungsgerät der Einrichtung (bei Fraunhofer Cisco PIX/ASA Firewall) lenkt diese Anfrage auf eine Webseite um, die zur Authentifizierung auffordert.

Der Fraunhofer-Mitarbeiter gibt dann seinen Benutzernamen und sein Passwort ein, das über eine verschlüsselte Leitung zu einem RADIUS-Server in der Einrichtung gesendet wird. Ist der REALM der Authentifizierungsanfrage für diesen RADIUS-Server unbekannt, leitet er die Anfrage an einen übergeordneten RADIUS-Server weiter. Die Anfrage wird dann so lange weitergeleitet, bis sie von den RADIUS-Servern des DFN an die zentralen RADIUS-Server der Fraunhofer-Gesellschaft gelangt. Diese leiten die Anfragen mit dem REALM *.fraunhofer.de dann ein letztes Mal an den Fraunhofer-Validator weiter, der die Anfrage beantwortet.

Eine Authentifizierungsanfrage besteht aus einem Benutzernamen *<User>@<REALM>* und einem Passwort. Diese werden im Folgenden beschrieben.

3.1 Benutzername

Als Benutzername wird beim Fraunhofer-Roaming die kanonische E-Mail-Adresse des Benutzers folgender Form verwendet:

<Vorname>.<Nachname>@<Institutskürzel>.fraunhofer.de

Die kanonische E-Mail-Adresse wird aus verschiedenen Gründen verwendet:

- Die Benutzer kennen ‚Ihre' persönliche E-Mail-Adresse. Es ist kein zusätzlicher Login-Name notwendig.
- Es existiert eine Vergaberichtlinie für die kanonische E-Mail-Adresse.
- Die kanonische E-Mail-Adresse eines Benutzers ist eindeutig.

3.2 Passwort

Bei der hier verwendeten Authentifizierung mittels Web-Redirect sieht jeder beteiligte Knoten das Passwort des Benutzers im Klartext. Die Verwendung des eigentlichen Benutzerpasswortes scheidet damit aus, da dieses in folgenden Kontexten benutzt wird:

- Arbeitsplatz-Authentifizierung
  Das eigentliche Benutzerpasswort wird zur Authentifizierung am Arbeitsplatz benutzt, wodurch dem Benutzer eine Fülle von Rechten zuteil wird.

- Remote-VPN-Zugang
  Für die Arbeit im Home-Office und auf Dienstreisen wird den Mitarbeitern die Möglichkeit gegeben, sich mit ihrem persönlichen Passwort zu authentifizieren.

Aufgrund der Signifikanz des Benutzerpasswortes und der Gefahr des Mit-Lauschens bei der Authentifizierung mittels Web-Redirect werden beim Fraunhofer-Roaming Einmal-Passworte verwendet. Diese werden im Folgenden genauer beschrieben.

4 Einmal-Passworte

Um den Fraunhofer-Mitarbeitern einen sicheren Zugang per Fraunhofer-Roaming anzubieten, werden Einmalpassworte verwendet. Über die Webseite

https://roaming.noc.fraunhofer.de

wird jedem Mitarbeiter mit einem gültigen Fraunhofer-.Zertifikat die Möglichkeit gegeben, sich eine Liste von 100 Passworten zu generieren. Der Zugriff zu dieser Webseite ist auf Fraunhofer-Interne Netzwerke beschränkt. Abbildung 4 zeigt die Webseite.

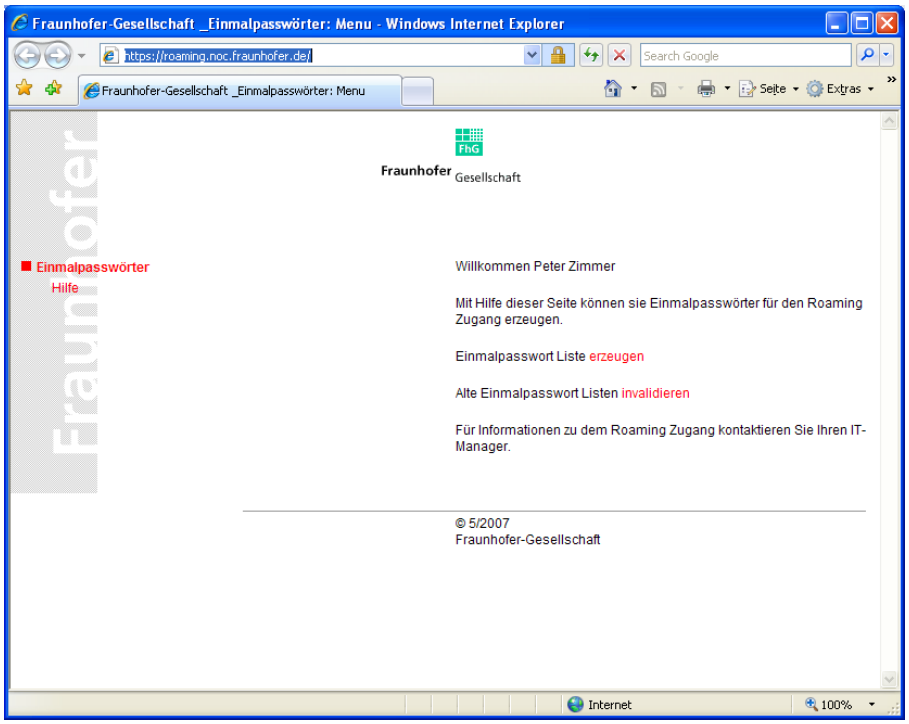
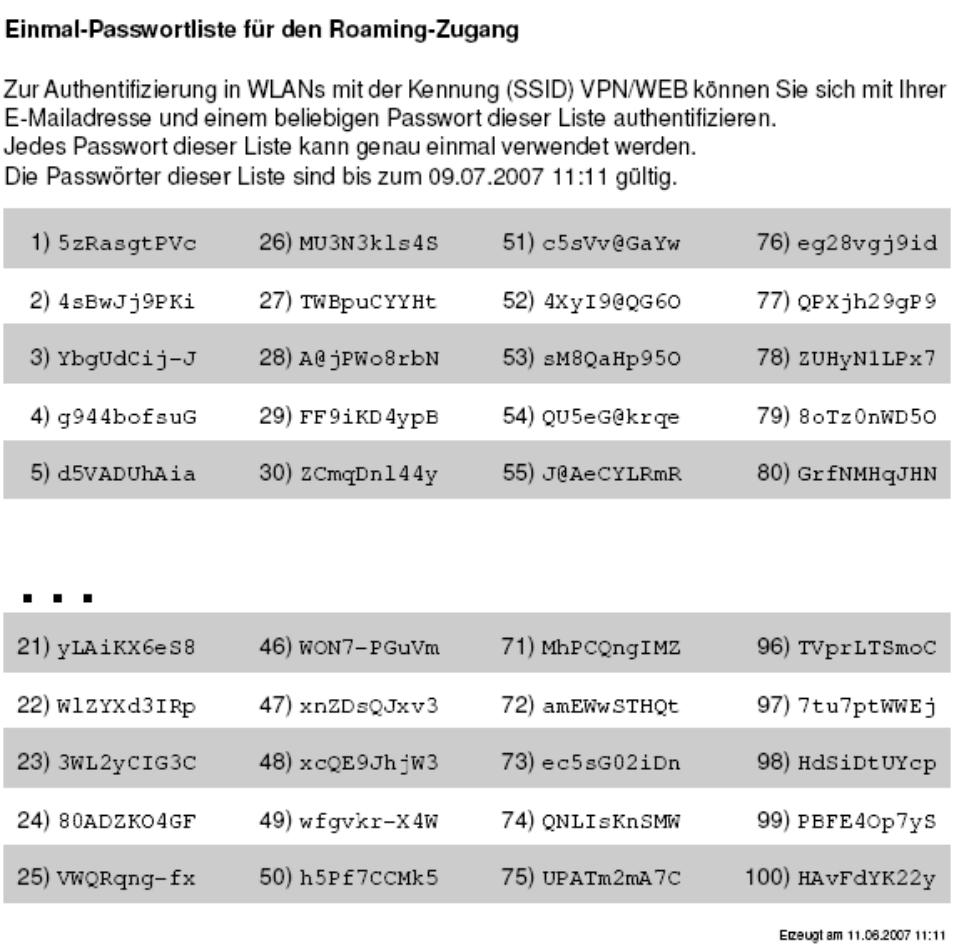


Abbildung 4: Webseite zur Erzeugung von Einmal-Passwortlisten

Die erzeugten Einmal-Passworte können nur genau einmal zur Authentifizierung verwendet werden und haben eine Gültigkeit von 4 Wochen. Nur die zuletzt erzeugte Einmal-Passwortliste ist gültig. Die Webseite bietet die Möglichkeit der manuellen Sperrung der aktiven Einmal-.Passwortliste.



Einmal-Passwortliste für den Roaming-Zugang

Zur Authentifizierung in WLANs mit der Kennung (SSID) VPN/WEB können Sie sich mit Ihrer E-Mailadresse und einem beliebigen Passwort dieser Liste authentifizieren.
Jedes Passwort dieser Liste kann genau einmal verwendet werden.
Die Passwörter dieser Liste sind bis zum 09.07.2007 11:11 gültig.

1) 5zRasgtPVc	26) MU3N3kls4S	51) c5sVv@GaYw	76) eg28vgj9id
2) 4sBwJj9PKi	27) TWBpuCYYHt	52) 4XyI9@QG6O	77) QPXjh29gP9
3) YbgUdCij-J	28) A@jPWo8rbN	53) sM8QaHp95O	78) ZUHyN1LPx7
4) g944bofsuG	29) FF9iKD4ypB	54) QU5eG@krqe	79) 8oTz0nWD5O
5) d5VADUhAia	30) ZCmqDnl44y	55) J@AeCYLRmR	80) GrfNMHqJHN

▪ ▪ ▪

21) yLAiKX6eS8	46) WON7-PGuVm	71) MhPCQngIMZ	96) TVprLTSmoC
22) WlZYXd3IRp	47) xnZDsQJxv3	72) amEWwSTHQt	97) 7tu7ptWWEj
23) 3WL2yCIG3C	48) xcQE9JhjW3	73) ec5sG02iDn	98) HdSiDtUYcp
24) 80ADZKO4GF	49) wfgvkr-X4W	74) QNLIsKnSMW	99) PBFE4Op7yS
25) VWQRqng-fx	50) h5Pf7CCMk5	75) UPATm2mA7C	100) HAvFdYK22y

Erzeugt am 11.06.2007 11:11

Abbildung 5: Einmal-Passwortliste

Abbildung 5 zeigt beispielhaft eine erzeugte Einmal-Passwortliste. Die einzelnen Zeilen sind durch eine Grauabstufung gut voneinander zu unterscheiden und jedes Passwort wird mit einer fortlaufenden Nummer versehen.

Die Nummerierung der Passworte wird derzeit nicht verwendet, da die benutzten Authentifizierungsgeräte (Cisco PIX/ASA [6]) ein Challenge-Verfahren nicht unterstützen.

4.1 Realisierung

Die Authentifizierung aller REALMS *.fraunhofer.de wird durch den RADIUS-Server auf dem Rechner roaming.noc.fraunhofer.de erledigt. Dieser authentifiziert mittels des ebenfalls auf diesem Rechner installierten Webservers. Der Webserver beinhaltet sowohl den Generator, mit dessen Hilfe die Benutzer Einmal-Passwortlisten erzeugen, als auch einen Validator, der für die Bearbeitung von Authentifizierungsanfragen zuständig ist. Der Generator ist per https aus allen Fraunhofer-Netzwerken zugänglich und der Validator ist per http ausschließlich von der lokalen Maschine (127.0.0.1) aus erreichbar. Abbildung 6 zeigt das Zusammenspiel der Komponenten auf roaming.noc.fraunhofer.de.

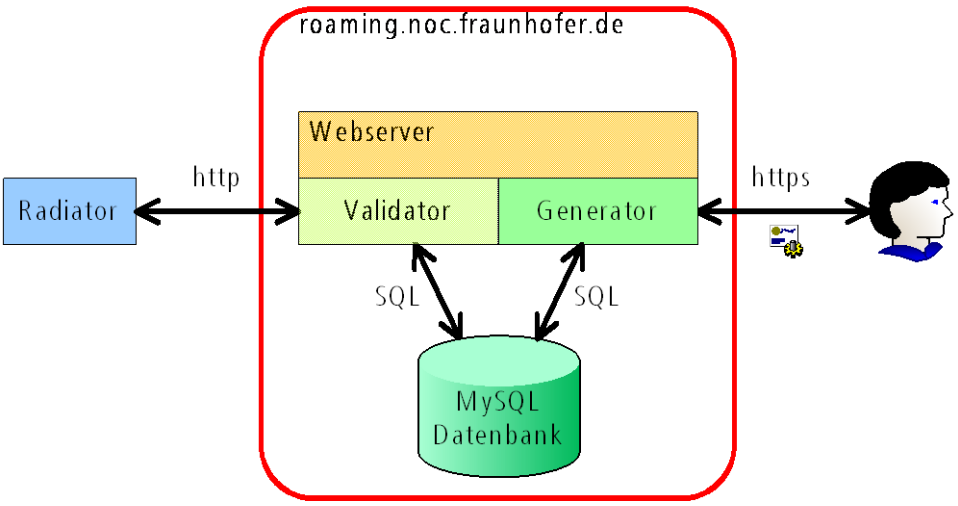


Abbildung 6: Aufbau von roaming.noc.fraunhofer.de

Erzeugt ein Benutzer eine Einmal-Passwortliste, schreibt der Generator diese als MD5-Hash in eine MySQL-Datenbank und löscht alle bestehenden Passwortlisten des Benutzers.

An roaming.noc.fraunhofer.de ankommende Authentifizierungsanfragen werden durch den RADIUS-Server an den Validator übermittelt. Die zuvor durch den Benutzer im Generator erzeugten Passworte sind als MD5-Hash in einer lokalen MySQL Datenbank gespeichert. Beim Eintreffen einer Authentifizierungsanfrage vergleicht der Validator die in der Authentifizierungsanfrage übergebenen Benutzerdaten mit denen in der Datenbank gespeicherten Daten.

Stimmen die Daten überein, gibt der Validator eine positive Nachricht an den lokalen RADIUS-Server zurück und invalidiert das verwendete Passwort.

Erhält der Validator ein falsches Passwort oder ist für den Benutzer kein Passwort hinterlegt oder existiert der Benutzer nicht, gibt er eine negative Nachricht an den lokalen RADIUS-Server zurück. Aus der Antwort geht nicht hervor, was der Grund für die Ablehnung der Authentifizierungsanfrage ist.

5 Ausblick

Der vorliegende Artikel beschreibt den derzeitigen Stand der Umsetzung von Fraunhofer-Roaming.

Alle Fraunhofer-Mitarbeiter mit einem gültigen Zertifikat können den Dienst in denen am DFNRoaming teilnehmenden Einrichtungen nutzen. Alle Fraunhofer-Institute mit WLAN sind *Roaming-Ready*. Durch wenige Handgriffe kann ein entsprechendes Angebot für die Gäste realisiert werden. Hier findet derzeit eine Kampagne statt, Fraunhofer-Roaming in den Fraunhofer-Instituten anzubieten.

In Fraunhofer-Roaming wird eine Authentifizierung mittels Web-Redirect-Verfahren mit Einmal-Passworten verwendet. Einmal-Passworte erscheinen hier notwendig, da beim Web-Redirect die Passworte im Klartext übertragen werden.

Derzeit ist eine Unterstützung für eine 802.1x/802.11i-basierte [8] Authentifizierung mit Integration der PKIv2-Zertifikate im Fraunhofer-Roaming in Arbeit. Damit wird die Authentifizierungskette verschlüsselt. Die genaue Spezifizierung ist derzeit in Arbeit. Das in diesem Dokument beschriebene Verfahren mittels Einmal-Passworten wird bis auf Weiteres unterstützt.

Aufgrund der zentralen Rolle des Validators und der MySQL-Datenbank, in der die Einmal-Passworte gespeichert sind, ist eine ausfallsichere Konfiguration dieser Komponenten in Arbeit. Der Webserver, auf dem der Validator und der Generator betrieben werden, wird redundant ausgelegt. Die MySQL-Datenbank wird mittels MySQL-Cluster ausfallsicher implementiert.

Neue AAA-Techniken wie z.B. Shibboleth [9] werden weiter beobachtet und bewertet, inwieweit ein Einsatz im Rahmen des Fraunhofer-Roaming in Frage kommt.

Quellenverzeichnis

[1] B.Kofler: DMZ Dienstemodellierung, 2006

[2] C. Rigney, S. Willens, A. Rubens, W. Simpson: IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), Juni 2000 1997

[3] J. Hassell: RADIUS, O'Reilly, 2003

[4] FreeRADIUS, the world's most popular RADIUS server, http://www.freeradius.org/, Juni 2007

[5] OSC Radiator RADIUS Software, http://www.open.com.au/radiator/index.html, Juni 2007

[6] Cisco ASA 5500 Series Adaptive Security Appliances, http://www.cisco.com/go/asa, Juni 2007

[7] IEEE Computer Society: 802.1X™ IEEE Standard for Local and Metropolitan Area Networks, Dezember 2004

[8] P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese: IETF RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, September 2003.

[9] Shibboleth Project Internet2 Middleware, http://shibboleth.internet2.edu/, Juni 2007